

HASIL CEK_60020397_Point-C31-IRD-850GB-Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:10AM (UTC+0700)

Submission ID: 1471661213

File name: ensik_Data_Recovery_Berbasis_Android_Menggunakan_Metode_NIST.pdf (1.55M)

Word count: 3910

Character count: 23834

PERBANDINGAN TOOL FORENSIK DATA RECOVERY BERBASIS ANDROID MENGUNAKAN METODE NIST

Imam Riadi¹, Sunardi², Sahiruddin³

¹Program Studi Sistem Informasi Universitas Ahmad Dahlan

²Program Studi Teknik Elektro Universitas Ahmad Dahlan

³Program Studi Teknik Informatika Universitas Ahmad Dahlan

Email: ¹imam.riadi@is.uad.ac.id, ²sunardi@mti.uad.ac.id, ³sahiruddinbuton@gmail.com

*Penulis Korespondensi

(Naskah masuk: 04 April 2019, diterima untuk diterbitkan: 14 Januari 2020)

Abstrak

2
Perkembangan *smartphone* tidak hanya memberikan dampak positif tetapi dapat berdampak negatif ketika dimanfaatkan untuk melakukan tindakan kejahatan. Saat ini terdapat banyak kasus penghapusan barang bukti kejahatan untuk menghilangkan jejak pelaku. Barang bukti yang telah dihapus menjadi problem bagi pihak berwajib untuk membuktikan kejahatan pelaku dalam persidangan. Penelitian ini bertujuan membandingkan kinerja *tool* forensik dalam mengembalikan data yang telah dihapus berupa data kontak, log panggilan, dan pesan yang digunakan sebagai barang bukti dalam persidangan. Penelitian ini menggunakan dua *smartphone* serta dua *tool* forensik Wondershare dr. Fone for Android dan Oxygen Forensics Suite 2014, dan menggunakan metode NIST yang memiliki kerangka kerja dan proses forensik terstruktur yang menjamin investigator mengikuti langkah penelitian agar hasilnya dapat dipertanggung jawabkan. Hasil penelitian ini bahwa Wondershare pada *smartphone* 1 berhasil mengembalikan data terhapus dengan persentase keberhasilan 31%, sementara Oxygen mencapai keberhasilan 67%. Pada *smartphone* 2 Wondershare berhasil mengembalikan data terhapus dengan persentase keberhasilan mencapai 35% dan Oxygen memiliki persentase keberhasilan 69%. Dari hasil yang diperoleh dapat disimpulkan bahwa Oxygen Forensics Suite 2014 memiliki kinerja yang baik daripada Wondershare dr. Fone for Android dalam mengembalikan data yang telah dihapus, dan bukti digital yang diperoleh dengan Oxygen dapat digunakan untuk menyelesaikan kasus kejahatan di persidangan.

Kata kunci: *forensic, recovery, android, NIST, Wondershare, Oxygen.*

FORENSIC TOOL COMPARISON DATA RECOVERY BASED ANDROID USING NIST METHOD

Abstract

The development of smartphones not only has a positive impact but can have a negative impact when it is used to commit a crime. At present, there are many cases of elimination of evidence of the crime to eliminate traces of perpetrators. Evidence that has been removed becomes a problem for the authorities to prove the crime of the perpetrators in the trial. This research aims to compare the performance of the forensic tool in returning deleted data in the form of contact data, call logs, and messages used as evidence in the trial. This research uses two smartphones as well as two Wondershare forensic tools from dr. Fone for Android and Oxygen Forensics Suite 2014, and use the NIST method which has a structured framework and forensic process that ensures investigators follow the steps of the research so that the results can be justified. The results of this research that Wondershare on smartphone 1 managed to restore deleted data with a success percentage of 31%, while Oxygen achieved 67% success. On Wondershare 2 smartphones, the data returned was deleted with a success rate of 35% and Oxygen having a success rate of 69%. From the results obtained it can be concluded that the Oxygen Forensics Suite 2014 has a good performance than Wondershare dr. Fone for Android in returning data that has been deleted, and digital evidence obtained with Oxygen can be used to resolve criminal cases in court.

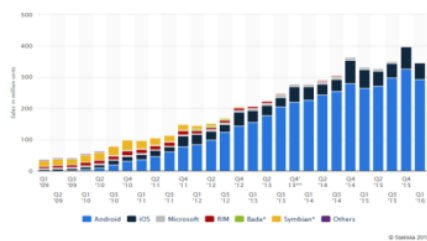
Keywords: *forensic, recovery, android, NIST, Wondershare, Oxygen.*

1. PENDAHULUAN

Perangkat seluler mengalami perkembangan yang sangat pesat seiring dengan perkembangan

11
teknologi (Guntur dkk, 2017). Salah satu bentuk teknologi yang perkembangannya dapat langsung dinikmati dan diaplikasikan dalam kehidupan sehari-hari adalah telepon genggam (*smartphone*).

Perangkat *smartphone* memiliki fungsi yang sama dengan komputer (Ruuhiwan dkk, 2017). *Smartphone* secara perlahan mulai menggantikan peran komputer dengan meningkatkan jumlah fitur dan aplikasi yang tersedia pada perangkat seluler (Rusydi dkk, 2018). *Smartphone* berbasis android termasuk salah satu jenis *smartphone* yang paling diminati dan memiliki banyak pengguna (Imam dkk, 2018). *Smartphone* diperkenalkan kepada publik pada tahun 2007 dan menjadi sistem operasi paling populer pada 2011, dilihat dari penjualan pada kuartal keempat 2016. Jumlah penjualan *smartphone* dengan sistem operasi Android adalah 379,98 juta unit (Rusydi dkk, 2017), statistik penjualan *smartphone* dengan berbagai sistem operasi seperti yang disajikan pada Gambar 1.



Gambar 1. Statistik penjualan *smartphone* dengan berbagai sistem operasi

perkembangan teknologi yang sangat signifikan terjadi pada telepon genggam yang dulu hanya dimanfaatkan untuk berkomunikasi via suara dan pesan singkat, handphone kini telah berinovasi dengan fitur-fitur yang disesuaikan keinginan pengguna. Bahkan perkembangan teknologi informasi saat ini sudah mulai mempengaruhi kegiatan dunia bisnis saham (Kennardi dkk, 2019).

Perkembangan teknologi tidak hanya membawa dampak positif tetapi, perkembangan teknologi memiliki sisi negatif. Salah satu dampak negatif yang dimaksud adalah ketika *smartphone* dimanfaatkan untuk tindakan yang melanggar hukum. Kejahatan yang dilakukan berupa penghapusan bukti digital pada *smartphone* untuk menghilangkan barang bukti tindakan kejahatan yang dilakukan oleh pelaku. Bukti digital ini berupa data yang ada pada *smartphone* seperti data kontak, log panggilan, pesan, video, gambar, dan dokumen yang akan dijadikan sebagai barang bukti kejahatan dalam persidangan (Sahiruddin dkk, 2018). Hal ini menjadi tantangan bagi forensika teknologi informasi dan penegak hukum untuk melakukan penyelidikan tersangka dalam sebuah kasus kejahatan karena bukti digital yang akan dijadikan sebagai barang bukti telah dihapus oleh pelaku.

Digital Forensik adalah proses ilmiah atau upaya ilmiah yang didasarkan pada ilmu mengumpulkan, menganalisis, dan menyajikan bukti dalam proses pengadilan untuk membantu pengungkapan kejahatan melalui pengungkapan bukti yang disahkan oleh hukum dan peraturan (Ade

dkk, 2017). *Live forensik* adalah metode forensik yang digunakan ketika sistem dalam kondisi berjalan. Hal ini karena data yang akan diambil kemungkinan hilang ketika sistem dimatikan. Implementasi *live forensik* biasanya digunakan dalam kasus *volatile memory*. Data yang mudah menguap adalah data yang biasanya disimpan di media sementara seperti RAM, yang datanya sangat mudah hilang (Muhammad dkk, 2017). Sifat bukti digital adalah rapuh, mudah menguap dan rentan jika tidak ditangani dengan benar. Semua jenis perubahan yang mengandung bukti digital akan mengarah pada kesimpulan yang salah, atau bukti tidak akan berguna (Faiz & Imam, 2017).

Penelitian ini bertujuan membandingkan kinerja dari *tool* forensik yang digunakan untuk mengembalikan data yang telah dihapus berupa data kontak, log panggilan, dan pesan pada perangkat *smartphone* yang akan dijadikan sebagai barang bukti untuk menyelesaikan kasus kejahatan penjualan narkoba dalam persidangan. Pengambilan barang bukti digital pada penelitian ini yaitu dengan menggunakan metode yang dikembangkan oleh *National Institute of Standard and Technology* (NIST) (Anton dkk, 2018). Hasil dari penelitian ini diharapkan dapat menambah pengetahuan di lingkup teknologi informasi khususnya pada bidang digital forensik dalam menyelesaikan kasus kejahatan.

Berita resmi kepolisian Republik Indonesia yang mengulas kasus-kasus penyalahgunaan *smartphone* antara lain:

1. Berita berjudul **Polisi Tangkap Tersangka Penipuan Via SMS Berkedok Korban Bencana Sulteng**, menceritakan penangkapan tersangka penipuan dengan modus penyebaran pesan singkat permintaan bantuan korban bencana alam Palu-Donggala. Tersangka menyebar SMS penipuan dengan menggunakan nomor 085338643339 bertuliskan "Tolong bantu keluarga kami korban Gempa Tsunami PALU-DONGGALA via Rekening BRI: 780601004778535 atas nama RISA RISTIANTI cabang BRI PALU-DONGGALA" (Farid, 2018).
2. Berita berjudul **Polisi Tangkap Warga Sleman Pembunuh Wanita di Bantul**, menceritakan tentang penangkapan seorang tersangka pembunuhan bernama Supriyono (48) yang dikenakan pasal pembunuhan berencana karena pelaku dianggap telah merencanakan penguasaan motor korban. Dari kasus ini polisi berhasil mengamankan sebuah *smartphone* yang di dalamnya terdapat pesan singkat janji untuk bertemu (Ahmad, 2018).
3. Berita berjudul **Polda Jawa Tengah Berhasil Menangkap Pelaku Penyebar Kampanye Hitam Melalui Pesan Singkat atau SMS (Short Message Service)**. Polisi berhasil menangkap tersangka penyebaran kampanye hitam salah satu pasangan peserta Pilkada Jawa Tengah berdasarkan laporan dari masyarakat setempat

tentang SMS yang masuk ke ponsel mereka (Admin,2018).

2. METODE PENELITIAN

Penelitian ini menggunakan metode yang mengacu pada proses investigasi yang digunakan oleh *National Institute of Standard and Technology* (NIST). Metode NIST terdiri dari 4 tahapan yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*. Skema metode NIST *mobile* forensik disajikan pada Gambar 2.



Gambar 2. Skema metode NIST *mobile* forensik

Penjelasan dari skema metode *National Institute of Standard and Technology* (NIST) adalah sebagai berikut:

1. *Collection/Preservation*

Tahap ini disebut juga tahap preservasi. *Collection* merupakan koleksi, atau identifikasi barang bukti yang digunakan berupa perangkat keras yang akan diambil datanya untuk digunakan sebagai bukti digital dari suatu kasus kejahatan digital. Proses ini dilakukan dengan mengikuti langkah pengamanan integritas data.

2. *Examination*

Examination merupakan proses pengambilan data pada barang bukti menggunakan *tool* forensik terpercaya sehingga data yang diperoleh memiliki integritas tinggi.

3. *Analysis*

Tahap ini adalah proses menganalisis dan mengevaluasi kembali data yang ditemukan dari hasil *examination*.

4. *Reporting*

Tahap *reporting* merupakan proses pelaporan hasil analisis yang meliputi informasi data yang berhasil ditemukan yang dijadikan sebagai laporan akhir proses forensik yang dilakukan.

2.1. Skenario Kasus

Simulasi ini mengangkat kasus tentang adanya laporan dari masyarakat mengenai sebuah tempat yang diduga sebagai tempat transaksi penjualan narkoba. Pihak yang berwajib segera menyikapi laporan tersebut dan melakukan pemeriksaan pada tempat kejadian perkara (TKP). Pemeriksaan yang dilakukan di TKP mendapatkan bukti berupa 2 unit *smartphone* yang diduga milik pelaku. *Smartphone* tersebut kemudian diamankan oleh pihak yang berwajib sebagai barang bukti.

Laboratorium forensik kemudian melakukan pemeriksaan terhadap *smartphone* tersebut dan

mendapatkan bukti awal berupa beberapa pesan dan log panggilan yang terindikasi tentang adanya transaksi penjualan narkoba pada *smartphone* tersebut. Tim laboratorium forensik kemudian melakukan tindakan forensik untuk melakukan *recovery* bukti digital yang mungkin telah dihapus oleh pelaku berupa percakapan untuk menguatkan bukti awal yang telah ditemukan.

Penelitian ini akan mengembalikan data yang telah dihapus berupa data kontak, log panggilan, dan pesan pada dua *smartphone* yang menjadi barang bukti. Pengambilan barang bukti berupa data yang telah dihapus menggunakan dua *tool* forensik yaitu Wondershare dr. Fone for Android dan Oxygen Forensic Suite 2014. Penggunaan kedua *smartphone* pada penelitian ini adalah untuk melihat kemampuan hasil *recovery* dari kedua *tool* yang di gunakan. Hasil penelitian kemudian disajikan dalam bentuk data kemampuan kinerja *tool* yang digunakan dalam mengembalikan data yang telah dihapus. Berikut adalah tabel data awal yang telah dihapus dalam simulasi kasus dari *smartphone* 1 dan *smartphone* 2.

Tabel 1. Data awal simulasi kasus *smartphone* 1

Barang Bukti 1		
No.	Jenis Data	Jumlah data
1	Kontak	13
2	Log Panggilan	12
3	Pesan	14

Informasi data yang dihapus dalam skenario kasus yang terdapat pada tabel 1 merupakan data *smartphone* 1 yang menjadi barang bukti terdiri dari 13 kontak, 12 log panggilan, dan 14 pesan.

Tabel 2. Data awal simulasi kasus *smartphone* 2

Barang Bukti 2		
No.	Jenis Data	Jumlah data
1	Kontak	10
2	Log Panggilan	11
3	Pesan	11

Informasi data yang dihapus dalam skenario kasus yang terdapat pada tabel 2 merupakan data *smartphone* 2 yang menjadi barang bukti yang terdiri dari 10 kontak, 11 log panggilan, dan 11 pesan.

Data awal simulasi kasus digunakan untuk mengetahui dan membandingkan hasil kinerja *tool* yang digunakan dalam mengembalikan data yang telah dihapus pada *smartphone* yang menjadi barang bukti.

2.2 Metode Perbandingan

Penelitian ini menggunakan perhitungan dengan angka indeks untuk menentukan kinerja masing-masing *tool* forensik sesuai dengan hasil *recovery tool*. Rumus perhitungan perbandingan angka indeks yang digunakan adalah indeks tidak tertimbang. Persamaan (1) merupakan penulisan persamaan

untuk mengetahui hasil kinerja *tool* forensik yang digunakan. Pada persamaan (1), P_{on} merupakan hasil persentase yang diharapkan, ΣP_n adalah data asli dari *smartphone*, sedangkan ΣP_o merupakan hasil akuisisi data menggunakan *tool* forensik (Anton dkk, 2018).

$$P_{on} = \frac{\Sigma P_n}{\Sigma P_o} \times 100\% \quad (1)$$

3. HASIL DAN PEMBAHASAN

3.1. Collection

Tahap *collection* merupakan pengumpulan bukti fisik yaitu barang bukti digital berupa perangkat *smartphone* yang diperlukan untuk melakukan proses penelitian. Penelitian ini menggunakan 2 barang bukti elektronik. *Smartphone* yang menjadi barang bukti seperti yang disajikan pada Gambar 3.



Gambar 3. *Smartphone* yang menjadi barang bukti

Proses *collection* juga akan mencatat spesifikasi dari barang bukti yang digunakan sebagai alat komunikasi transaksi penjualan narkoba. Berikut adalah tabel spesifikasi barang bukti yang digunakan.

Tabel 3. Spesifikasi barang bukti yang digunakan

Spesifikasi	Barang bukti 1	Barang bukti 2
Model	J5 2015	J1 Ace
Nomor Model	SM-J500G	SM-J111F
OS	Android	Android
Versi O	5.1 (Lollipop)	5.1 (Lollipop)

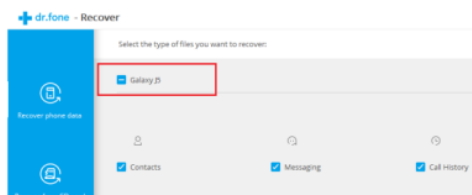
3.2. Examination

Tahap ini merupakan tahap pemeriksaan dan pengambilan data dari *smartphone* untuk memperoleh data yang telah dihapus pada barang bukti. Proses ekstraksi data yang dilakukan yaitu *smartphone* yang menjadi barang bukti harus terlebih dahulu terkoneksi pada laptop tempat kedua *tool* forensik di-install. Barang bukti 1 yang telah terkoneksi oleh Wondershare disajikan pada Gambar 4 dan barang bukti 2 yang terkoneksi dengan Wondershare disajikan pada Gambar 5.

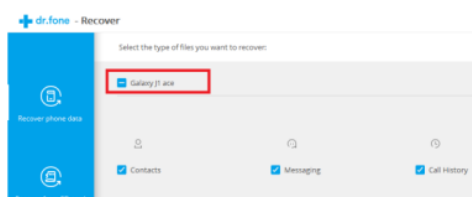
Tampilan pada Gambar 4 menunjukkan bahwa *smartphone* dengan tipe Samsung J5 telah terkoneksi dengan *tool* Wondershare, dan tampilan pada gambar 5 menunjukkan bahwa *smartphone* dengan tipe Samsung J1 Ace telah terkoneksi dengan *tool* Wondershare.

Selain informasi koneksi dari kedua *smartphone* tersebut, Wondershare juga memberikan kemudahan kepada pengguna untuk menentukan pilihan data

yang akan dikembalikan. Pada tampilan Gambar 4 dan Gambar 5 terdapat 3 jenis pilihan data yang akan dikembalikan yaitu data kontak, log panggilan, dan pesan.



Gambar 4. Barang bukti 1 yang telah terkoneksi oleh Wondershare



Gambar 5. Barang bukti 2 yang telah terkoneksi oleh Wondershare

Berbeda dengan Wondershare, koneksi barang bukti dengan *tool* Oxygen tidak memberikan informasi tentang jenis data yang akan dikembalikan. Barang bukti 1 yang telah terkoneksi oleh Oxygen seperti yang disajikan pada Gambar 6, dan Barang bukti 2 yang terkoneksi dengan Oxygen seperti yang disajikan pada Gambar 7.



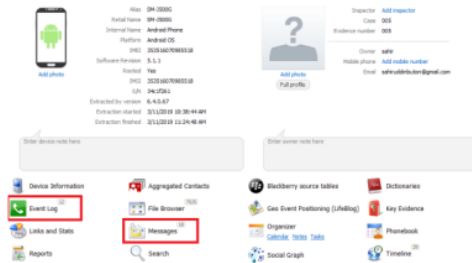
Gambar 6. Barang bukti 1 yang telah terkoneksi oleh Oxygen

Koneksi barang bukti dengan Oxygen hanya memberikan informasi tentang model, IMEI, *hardware revision*, dan *software revision* barang bukti.

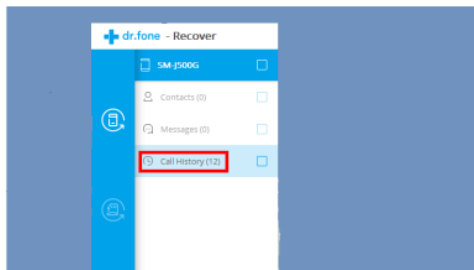
Setelah *smartphone* terkoneksi dengan kedua *tool* forensik yang digunakan, selanjutnya yaitu proses ekstraksi data yang telah dihapus pada *smartphone*. Lama waktu yang dibutuhkan untuk mengekstrak data disesuaikan dengan banyaknya data yang terhapus. Hasil ekstraksi dari barang bukti 1 oleh Wondershare seperti yang disajikan pada Gambar 8, dan hasil ekstraksi pada barang bukti 2 seperti yang disajikan pada Gambar 9.



Gambar 7. Barang bukti 2 yang telah terkoneksi oleh Oxygen

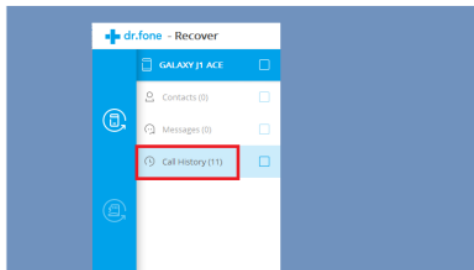


Gambar 10. Hasil ekstraksi dari barang bukti 1 oleh Oxygen



Gambar 8. Hasil ekstraksi dari barang bukti 1 oleh Wondershare

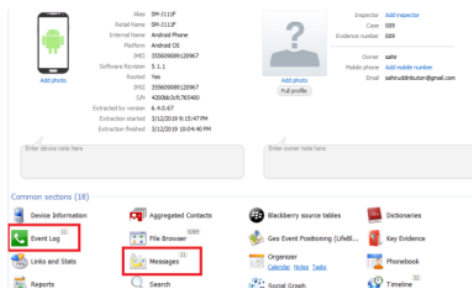
Hasil ekstraksi barang bukti 1 oleh Wondershare hanya berhasil mengembalikan data terhapus berupa 12 log panggilan, sementara data kontak dan pesan tidak dapat dikembalikan.



Gambar 9. Hasil ekstraksi dari barang bukti 2 oleh Wondershare

Hasil ekstraksi pada barang bukti 2 oleh Wondershare hanya berhasil mengembalikan data terhapus berupa 12 log panggilan, sementara data kontak dan pesan tidak dapat dikembalikan.

Hasil berbeda ditunjukkan oleh Oxygen yaitu data terhapus lebih banyak dikembalikan dibandingkan dengan hasil ekstraksi dengan Wondershare. Hasil ekstraksi barang bukti 1 oleh Oxygen seperti yang disajikan pada Gambar 10, dan hasil ekstraksi oleh Oxygen pada barang bukti 2 seperti yang disajikan pada Gambar 11.



Gambar 11. Hasil ekstraksi dari barang bukti 2 oleh Oxygen

Hasil ekstraksi pada barang bukti 2 oleh Oxygen berhasil mengembalikan data terhapus berupa 11 log panggilan dan 21 pesan, sementara data kontak tidak dapat dikembalikan.

3.3. Analysis

Hasil analisis dari masing-masing *tool* ini dapat menjadi bukti bahwa data yang telah dihapus pada *smartphone* masih dapat di-*recovery* sehingga menjadi data pendukung pada penyelesaian suatu kasus kejahatan.

Hasil *examination* data yang telah dihapus menggunakan *tool* Wondershare hanya dapat mengembalikan data berupa log panggilan, sementara data kontak dan pesan tidak dapat dikembalikan. Data terhapus yang berhasil dikembalikan oleh Wondershare pada barang bukti 1 dapat dilihat pada Gambar 12, dan Data terhapus yang berhasil dikembalikan Wondershare pada barang bukti 2 dapat dilihat pada Gambar 13.

Jumlah data terhapus yang berhasil dikembalikan berupa log panggilan oleh Wondershare pada barang bukti 1 memiliki jumlah yang sama dengan data yang dihapus pada simulasi kasus yaitu sebanyak 12 log panggilan. Data kontak dan pesan tidak memperoleh hasil apapun.

Contact	Date	Type	Duration
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00

Gambar 12. Data terhapus yang berhasil dikembalikan Wondershare pada barang bukti 1

Contact	Date	Type	Duration
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00

Gambar 13. Data terhapus yang berhasil dikembalikan Wondershare pada barang bukti 2

Jumlah data terhapus yang berhasil dikembalikan berupa log panggilan oleh Wondershare pada barang bukti 2 memiliki jumlah yang sama dengan data yang dihapus pada simulasi kasus yaitu sebanyak 11 log panggilan. Data kontak dan pesan tidak memperoleh hasil apapun.

Hasil examination data yang telah dihapus menggunakan tool Oxygen dapat mengembalikan data berupa log panggilan dan pesan, sementara data kontak tidak dapat dikembalikan. Data terhapus yang berhasil dikembalikan oleh Oxygen pada barang bukti 1 disajikan pada gambar 14, dan data terhapus yang berhasil dikembalikan Oxygen pada barang bukti 2 disajikan pada gambar 15.

Jumlah data terhapus yang berhasil dikembalikan berupa log panggilan oleh Oxygen pada barang bukti 1 memiliki jumlah yang sama dengan data yang dihapus pada simulasi kasus yaitu sebanyak 12 log panggilan. Data berbeda ditunjukkan oleh data pesan yang berhasil dikembalikan yaitu sebanyak 18 pesan dari 14 data yang dihapus pada simulasi kasus. Hasil analisis menunjukkan bahwa tambahan data sebanyak 4 pesan merupakan pesan yang sama atau pesan gagal yang dianggap sebagai satu data temuan oleh Oxygen.

Berbeda dengan hasil recovery pada data log panggilan dan pesan terhapus yang dapat dikembalikan oleh Oxygen, hasil recovery data kontak tidak memberikan hasil yang diharapkan karena data yang telah dihapus pada barang bukti 1 tidak dapat dikembalikan. Hal ini berlaku juga pada barang bukti 2 yaitu data log panggilan dan pesan yang telah dihapus masih dapat dikembalikan oleh Oxygen, sementara data kontak yang telah dihapus tidak dapat dikembalikan.

Contact	Date	Type	Duration
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00

Gambar 14. Data terhapus yang berhasil dikembalikan Oxygen pada barang bukti 1

Contact	Date	Type	Duration
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00
WHS 3	3/11/2019 10:17:25 AM	Outgoing	00:00:00

Gambar 15. Data terhapus yang berhasil dikembalikan Oxygen pada barang bukti 2

Jumlah data terhapus yang berhasil dikembalikan berupa log panggilan oleh Oxygen pada barang bukti 2 memiliki jumlah yang sama dengan data yang dihapus pada simulasi kasus yaitu sebanyak 11 log panggilan. Data berbeda ditunjukkan oleh data pesan yang berhasil dikembalikan yaitu sebanyak 21 pesan dari 11 data yang dihapus pada simulasi kasus. Hasil analisis menunjukkan bahwa tambahan data sebanyak 10 pesan merupakan pesan yang sama atau pesan gagal yang dianggap sebagai satu data temuan oleh Oxygen. Data kontak pada barang bukti 2 juga tidak memperoleh hasil apapun.

3.4. Reporting

Hasil analisis forensik yang dilakukan dari 3 jenis data yang menjadi fokus pengembalian data (data kontak, log panggilan, dan pesan), Wondershare berhasil mengembalikan 1 jenis data yang telah dihapus, sedangkan Oxygen berhasil mengembalikan 2 jenis data yang telah dihapus. Berikut adalah tabel hasil *recovery* dari 2 *tool* forensik pada *smartphone* 1 dan *smartphone* 2.

Tabel 4. Hasil *recovery* dari 2 *tool* forensik pada *smartphone* 1

Smartphone 1			
Tool forensik	Bukti digital	Data asli smartphone	Data recovery tool forensik
Wondershare	kontak	13	0
	Log panggilan	12	12
	pesan	14	0
Oxygen	kontak	13	0
	Log panggilan	12	12
	Pesan	14	14

Perbandingan hasil kinerja *tool* dari *smartphone* 1 menggunakan Wondershare dan oxygen adalah Wondershare memiliki hasil kinerja 31% dalam mengembalikan data terhapus, sedangkan dengan Oxygen forensik mencapai 67%. Hasil ini didapatkan menggunakan perhitungan perbandingan angka indeks tidak tertimbang sebagai berikut:

Perhitungan kinerja *tool* menggunakan Wondershare

$$\text{Hasil kinerja tool} = \frac{12}{39} \times 100\% = 31\%$$

Perhitungan kinerja *tool* menggunakan Oxygen

$$\text{Hasil kinerja tool} = \frac{26}{39} \times 100\% = 67\%$$

Tabel 5. Hasil *recovery* dari 2 *tool* forensik pada *smartphone* 2

Smartphone 2			
Tool forensik	Bukti digital	Data asli smartphone	Data recovery tool forensik
Wondershare	kontak	10	0
	Log panggilan	11	11
	pesan	11	0
Oxygen	kontak	10	0
	Log panggilan	11	11
	Pesan	11	11

Perbandingan hasil kinerja *tool* dari *smartphone* 2 yang menjadi barang bukti menggunakan Wondershare dan oxygen adalah Wondershare memiliki hasil kinerja 35% dalam mengembalikan data terhapus, sedangkan hasil yang diperoleh dengan Oxygen forensik adalah 69%. Hasil ini didapatkan menggunakan perhitungan perbandingan angka indeks tidak tertimbang sebagai berikut:

Perhitungan kinerja *tool* menggunakan Wondershare

$$\text{Hasil kinerja tool} = \frac{11}{32} \times 100\% = 35\%$$

Perhitungan kinerja *tool* menggunakan Oxygen

$$\text{Hasil kinerja tool} = \frac{22}{32} \times 100\% = 69\%$$

Berdasarkan perbandingan hasil yang diperoleh menggunakan 2 *tool* forensik Wondershare dan Oxygen pada 2 *smartphone* yang menjadi barang bukti maka dapat diketahui bahwa hasil *recovery* data yang telah dihapus dengan *tool* Oxygen lebih signifikan dibandingkan dengan Wondershare.

4. KESIMPULAN

Berdasarkan hasil penelitian tentang perbandingan *tool* forensik untuk menemukan bukti digital yang telah dihapus menggunakan *tool* Wondershare dan Oxygen pada 2 *smartphone* memberikan kesimpulan bahwa pada *smartphone* 1 hasil kinerja *tool* Wondershare hanya mencapai 31% data terhapus dapat dikembalikan, sedangkan hasil kinerja dengan Oxygen forensik mencapai 67%.

Pada *smartphone* 2 hasil kinerja *tool* Wondershare hanya mencapai 35% data terhapus dapat dikembalikan, sedangkan dengan Oxygen forensik mencapai 69%. Dengan demikian data hasil *recovery* bukti digital dengan *tool* Oxygen sangat direkomendasikan sebagai barang bukti dalam membuktikan kasus kejahatan dalam persidangan. Untuk pengembangan pada penelitian berikutnya dapat ditambahkan dengan *smartphone* dan sistem operasi yang berbeda sehingga hasil yang diperoleh menjadi tolak ukur yang baik dari perbandingan performa kinerja kedua *tool* yang digunakan.

DAFTAR PUSTAKA

- ADE, K., IMAM, R. & AHMAD, L., 2017. Forensic Analysis and Prevent of CrossSiteScripting inSingleVictim Attack Using Open Web Application Security Project (OWASP) Framework. *Journal of Theoretical and Applied Information Technology (JATIT)*, Volume 95, pp. 1363-1371.
- ADMIN, 2018. *Polda Jawa Tengah Berhasil Menangkap Pelaku Penyebar Kampanye Hitam Melalui Pesan singkat atau SMS (Short Message Service)*. [Online] Available at: <https://www.cnnindonesia.com/pilkadasere ntak/nasional/20180627124049-12-309424> [Diakses 12 12 2018].Ahmad, S., t.thn. [Online].
- AHMAD, S., 2018. *Polisi Tangkap Warga Sleman Pembunuh Wanita di Bantul*. [Online] Available at: <http://tribatanews.polri.go.id/?p=411013> [Diakses 12 12 2018].
- ANTON, Y., IMAM, R. & IKHWAN, A., 2018. Identification of Digital Evidence Facebook Messenger on Mobile Phone With National Institute of Standards Technology (NIST) Method. *KURSOR Journal*, Volume 9, pp. 111-118.

- ANTON, Y., IMAM, R. & MUHAMAD, F. P. C., 2018. Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal Informatics*, Volume 5, pp. 235-247.
- FAIZ, A. & IMAM, R., ⁷2017. Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security (IJCSIS)*, Volume 15, pp. ¹⁰173-178.
- FARID, A., 2018. *Polisi Tangkap Tersangka Penipuan Via SMS Berkedok Korban Bencana Sulteng*. [Online] Available at: <http://tribrataneews.polri.go.id/?p=411013> [Diakses 12 12 2018].
- GUNTUR, Z. M., RUSYDI, U. & IMAM, R., 2017. *Analisis Forensik Aplikasi Instant Messaging Berbasis Android*. In *Prosiding Annual Research Seminar* (Vol 2, pp 102-105).
- IMAM, R., RUSYDI, U. & ARIZONA, F., 2018. Forensic Tools Performance Analysis on Android Based Blackberry Messenger Using NIST Measurement. *International Journal of Electrical and Computer Engineering*, Volume 8, pp. 3991-4003.
- KENNARDI, T. D., MURTIYANTO, S., RAYMOND, S. & RESMANA, L., 2019. Sistem Notifikasi SMS Hasil Prediksi Saham/Forex Menggunakan Rasberry PI. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, Volume 6, pp. 113-122.
- MUHAMMAD, M. I., IMAM, R. & AHAMD, L., 2017. Live Forensics on RouterOS using API Servicesto Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, Volume 15, pp. 406-410.
- RUSYDI, U., IMAM, R. & GUNTUR, Z. M., 2017. A Comparative Study of Forensic Tools for Measurements. *International Journal Of Advanced Computer Science And Applications*, Volume 8, pp. 69-75.
- RUSYDI, U., IMAM, R. & GUNTUR, Z. M., 2018. Mobile Forensic Tools Evaluation for Digital Crime Investigation. *International Journal on Advanced Science, Engineering and Information Technology*, Volume 8, pp. 949-955.
- RUUHWAN, IMAM, R. & YUDI, P., 2017. Evaluation of Integrated Digital Forensics Investigation of Smartphone Using Soft System Methodology. *Intenational Journal of Electrical and Computer Engineering (IJECE)*, Volume 7, pp. 2806-2817.
- SAHIRUDDIN, IMAM, R. & SUNARDI, 2018. *Data Recovery Dengan Keamanan Fingerprint Pada Smartphone Android*. In *Prosiding SENDI_U*, pp 140-144.

HASIL CEK_60020397_Point-C31-IRD-850GB-Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST

ORIGINALITY REPORT

9%

SIMILARITY INDEX

6%

INTERNET SOURCES

2%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1

core.ac.uk

Internet Source

2%

2

www.researchgate.net

Internet Source

1%

3

Submitted to Universitas Brawijaya

Student Paper

1%

4

Submitted to Universitas Islam Riau

Student Paper

1%

5

journal.ithb.ac.id

Internet Source

1%

6

doku.pub

Internet Source

1%

7

ejournal.unira.ac.id

Internet Source

1%

8

Submitted to Universitas Atma Jaya Yogyakarta

Student Paper

1%

9	Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar. "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)", J-SAKTI (Jurnal Sains Komputer dan Informatika), 2020 Publication	1%
---	--	----

10	tribratanews.polri.go.id Internet Source	1%
----	---	----

11	jurnal.unmuhjember.ac.id Internet Source	1%
----	---	----

Exclude quotes	On
Exclude bibliography	On

Exclude matches	< 1%
-----------------	------